ASA:使用ASDM的智慧隧道配置示例

目錄

簡介

智慧隧道是基於TCP的應用程式與專用站點之間的連線，它使用無客戶端（基於瀏覽器）的SSL VPN會話作為路徑，使用安全裝置作為代理伺服器。您可以標識要向其授予智慧隧道訪問許可權的應用程式，並指定每個應用程式的本地路徑。對於在Microsoft Windows上運行的應用程式，您還可以要求將校驗和的SHA-1雜湊匹配作為授予智慧隧道訪問許可權的條件。

*Lotus SameTime*和*Microsoft Outlook Express*是您可能要授予智慧隧道訪問許可權的應用程式的示例。

取決於應用程式是客戶端還是支援Web的應用程式，智慧隧道配置需要以下過程之一：

- 建立客戶端應用程式的一個或多個智慧隧道清單，然後將清單分配給要為其提供智慧隧道訪問的組策略或本地使用者策略。
- 建立一個或多個書籤清單條目，指定符合智慧隧道訪問的啟用Web的應用程式的URL，然後將清單分配給要為其提供智慧隧道訪問的DAP、組策略或本地使用者策略。您還可以列出啟用Web的應用程式，以便通過無客戶端SSL VPN會話在智慧隧道連線中自動提交登入憑證。

本檔案假設Cisco AnyConnect SSL VPN客戶端配置已建立且工作正常，以便可以在現有配置上配置智慧隧道功能。有關如何配置Cisco AnyConnect SSL VPN客戶端的詳細資訊，請參閱ASA 8.x:在ASA配置上允許對AnyConnect VPN客戶端進行分割隧道的示例。

注意：確保*ASA 8.x的*使用ASDM 6.0(2)的ASA配置部分中所述的步驟4.b到4.l:*在ASA上為AnyConnect VPN客戶端執行允許切分*隧道的配置示例不是為了配置智慧隧道功能。

本文檔介紹如何在Cisco ASA 5500系列自適應安全裝置上配置智慧隧道。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本8.0(2)的Cisco ASA 5500系列自適應安全裝置
- 運行Microsoft Vista、Windows XP SP2或Windows 2000 Professional SP4（帶有Microsoft Installer 3.1版）的PC
- 思科調適型安全裝置管理員(ASDM)版本6.0(2)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

智慧通道存取組態

智慧隧道表顯示智慧隧道清單，每個清單標識一個或多個符合智慧隧道訪問條件的應用程式及其關聯的作業系統(OS)。 由於每個組策略或本地使用者策略都支援一個智慧隧道清單，因此必須將要支援的基於非瀏覽器的應用程式分組到一個智慧隧道清單中。配置清單後，可以將其分配給一個或多個組策略或本地使用者策略。

使用智慧隧道視窗(**Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**)可以完成以下步驟：

- **新增智慧隧道清單並將應用程式新增到清單**完成以下步驟，以便新增智慧隧道清單並將應用程式新增到清單中：按一下「**Add**」。系統將顯示Add Smart Tunnel List對話方塊。輸入清單的名稱，然後按一下**Add**。ASDM將開啟Add Smart Tunnel Entry對話方塊，通過該對話方塊，您可以將智慧隧道的屬性分配給清單。為智慧隧道分配所需屬性後，按一下**確定**。ASDM在清單中顯示這些屬性。根據需要重複這些步驟以完成清單，然後在Add Smart Tunnel List對話方塊中按一下**OK**。
- **更改智慧隧道清單**完成以下步驟即可變更智慧通道清單：按兩下該清單或選擇表中的清單，然後按一下**Edit**。按一下**Add**將一組新的智慧隧道屬性插入清單，或在清單中選擇一個條目，然後按一下**Edit**或**Delete**。

- **刪除清單**要刪除清單，請選擇表中的清單，然後按一下**刪除**。
- **新增書籤**在配置和分配智慧隧道清單之後，您可以通過為服務新增書籤並點選Add or Edit Bookmark對話方塊中的**Enable Smart Tunnel**選項來使智慧隧道易於使用。

智慧隧道訪問允許基於TCP的客戶端應用程式使用基於瀏覽器的VPN連線來連線服務。與外掛和傳統埠轉發技術相比，它為使用者提供了以下優勢：

- 智慧隧道比外掛具有更好的效能。
- 與埠轉發不同，智慧隧道無需將本地應用程式連線到本地埠，從而簡化了使用者體驗。
- 與埠轉發不同，智慧隧道不需要使用者具有管理員許可權。

智慧隧道要求、限制和限制

一般要求和限制

智慧隧道具有以下一般要求和限制：

- 發起智慧隧道的遠端主機必須運行32位版本的Microsoft Windows Vista、Windows XP或Windows 2000;或Mac OS 10.4或10.5。
- 智慧隧道自動登入僅支援Windows上的Microsoft Internet Explorer。
- 瀏覽器必須使用Java、Microsoft ActiveX或兩者同時啟用。
- 智慧隧道僅支援位於運行Microsoft Windows的電腦和安全裝置之間的代理。智慧隧道使用Internet Explorer配置（即Windows中用於系統範圍的配置）。 如果遠端電腦需要代理伺服器來訪問安全裝置，則連線的終止端的URL必須位於從代理服務排除的URL清單中。如果代理配置指定發往ASA的流量通過代理，則所有智慧隧道流量都通過代理。在基於HTTP的遠端訪問方案中，有時子網不提供使用者對VPN網關的訪問。在這種情況下，放置在ASA前方、用於在Web和終端使用者位置之間路由流量的代理提供Web訪問。但是，只有VPN使用者才能配置放置在ASA前面的代理。執行此操作時，他們必須確保這些代理支援CONNECT方法。對於需要身份驗證的代理，智慧隧道僅支援基本摘要式身份驗證型別。
- 當智慧隧道啟動時，安全裝置將隧道從瀏覽器處理使用者用於啟動無客戶端會話的所有流量。如果使用者啟動瀏覽器進程的另一個例項，它會將所有流量傳遞到隧道。如果瀏覽器進程相同，且安全裝置不提供對給定URL的訪問，則使用者無法開啟它。作為解決方法，使用者可以使用與用於建立無客戶端會話的瀏覽器不同的瀏覽器。
- 有狀態故障切換不會保留智慧隧道連線。使用者必須在故障轉移後重新連線。

Windows要求和限制

以下要求和限制僅適用於Windows:

- 只有Winsock 2、基於TCP的應用程式才有資格進行智慧隧道訪問。
- 安全裝置不支援Microsoft Outlook Exchange(MAPI)代理。埠轉發和智慧隧道都不支援MAPI。對於使用MAPI協定的Microsoft Outlook Exchange通訊，遠端使用者必須使用AnyConnect。
- 使用智慧隧道或埠轉發的Microsoft Windows Vista使用者必須將ASA的URL新增到受信任的站點區域。若要訪問「受信任的站點」區域，請啟動Internet Explorer，然後選擇**「工具」>「Internet選項」**，然後按一下**安全**頁籤。Vista使用者還可以禁用保護模式以便於智慧隧道訪問；但是，思科建議不要使用此方法，因為它會增加攻擊漏洞。

Mac OS要求和限制

以下要求和限制僅適用於Mac OS:

- Safari 3.1.1或更高版本或Firefox 3.0或更高版本
- Sun JRE 1.5或更高版本
- 只有從門戶頁面啟動的應用程式才能建立智慧隧道連線。此要求包括對Firefox的智慧隧道支援。在首次使用智慧隧道期間，使用Firefox啟動另一個Firefox例項需要名為csco_st的使用者配置檔案。如果此使用者配置檔案不存在，會話將提示使用者建立一個。
- 使用動態連結到SSL庫的TCP的應用程式可以通過智慧隧道工作。
- 智慧隧道不支援Mac OS上的以下功能和應用：代理服務自動登入使用兩級名稱空間的應用程式基於控制檯的應用，如Telnet、SSH和cURL使用dlopen或dlsym查詢libsocket呼叫的應用程式通過靜態連結應用程式查詢libsocket呼叫

設定

本節提供用於設定本文件中所述功能的資訊。

新增或編輯智慧隧道清單

通過Add Smart Tunnel List對話方塊，您可以將智慧隧道條目的清單新增到安全裝置配置中。通過Edit Smart Tunnel List對話方塊可以修改清單的內容。

欄位

清單名稱 — 為應用程式或程式清單輸入唯一名稱。名稱中的字元數沒有限制。請勿使用空格。在配置智慧隧道清單後，清單名稱顯示在無客戶端SSL VPN組策略和本地使用者策略中的智慧隧道清單屬性旁邊。指定有助於將其內容或用途與您可能配置的其他清單區分開的名稱。

新增或編輯智慧隧道條目

通過新增或編輯智慧隧道條目對話方塊，可以在智慧隧道清單中指定應用的屬性。

- **應用程式ID** — 輸入字串，以在智慧隧道清單中命名條目。該字串對於OS是唯一的。通常，它會命名要授予智慧隧道訪問的應用程式。為了支援選擇為其指定不同路徑或雜湊值的應用程式的多個版本，可以使用此屬性來區分條目，指定作業系統以及每個清單條目所支援的應用程式的名稱和版本。字串最多可以包含64個字元。
- **進程名**稱 — 輸入應用程式的檔名或路徑。字串最多可以包含128個字元Windows需要將此值與遠端主機上應用程式路徑的右側完全匹配才能使應用程式符合智慧隧道訪問的條件。如果只為Windows指定檔名，SSL VPN不會在遠端主機上實施位置限制來使應用程式符合智慧隧道訪問條件。如果指定路徑且使用者將應用程式安裝在另一個位置，則該應用程式不符合條件。只要字串的右側與您輸入的值相匹配，應用程式就可以駐留在任何路徑上。若要授權用於智慧隧道訪問的應用程式（如果該應用程式出現在遠端主機上的多個路徑之一），請在此欄位中僅指定應用程式的名稱和擴展，或者為每個路徑建立一個唯一的智慧隧道條目。對於Windows，如果要將智慧隧道訪問新增到從命令提示符啟動的應用程式，必須在智慧隧道清單中某條項的進程名稱中指定「cmd.exe」，並在另一條項中指定該應用程式本身的路徑，因為「cmd.exe」是應用程式的父項。Mac OS需要該進程的完整路徑，並且區分大小寫。為了避免為每個使用者名稱指定路徑，請在部分路徑（例如~/bin/vnc）前插入一個顎化符(~)。
- **OS** — 按一下Windows或Mac以指定應用程式的主機作業系統。
- **Hash** -(*可選，僅適用於Windows*)要獲取此值，請在使用SHA-1演算法計算雜湊的實用程式中輸

入執行檔的校驗和。Microsoft File Checksum Integrity Verifier(FCIV)便是此類實用程式的示例。在Availability and description of the File Checksum Integrity Verifier utility中提供了此工具。安裝FCIV後，將應用程式的臨時副本放在不包含空格的路徑上(例如c:/fciv.exe)，然後在命令列輸入fciv.exe -sha1應用程式（例如fciv.exe -sha1 c:\msimn.exe）以顯示SHA-1雜湊。SHA-1雜湊值始終為40個十六進位制字元。在授權應用進行智慧隧道訪問之前，無客戶端SSL VPN會計算與應用ID匹配的應用的雜湊值。如果結果與雜湊值匹配，則對應用程式進行智慧隧道訪問。輸入雜湊可以合理保證SSL VPN不會限定與您在應用程式ID中指定的字串相匹配的非法檔案。由於校驗和隨應用程式的每個版本或補丁而異，因此您輸入的雜湊只能與遠端主機上的一個版本或補丁匹配。要為應用程式的多個版本指定雜湊，請為每個雜湊值建立一個唯一的智慧隧道條目。**注意：如**果您輸入雜湊值，並且希望支援具有智慧隧道訪問許可權的應用程式的未來版本或修補程式，則必須以後更新智慧隧道清單。智慧隧道訪問突然出現問題，可能表示包含雜湊值的應用程式在應用程式升級時不是最新的。您可以通過不輸入雜湊值來避免此問題。

- 配置智慧隧道清單後，必須將其分配到組策略或本地使用者策略才能使其啟用，如下所示：要將清單分配給組策略，請選擇**Config > Remote Access VPN> Clientless SSL VPN Access > Group Policies > Add or Edit > Portal**，然後從Smart Tunnel List屬性旁的下拉選單中選擇智慧隧道名稱。要將清單分配給本地使用者策略，請選擇**Config > Remote Access VPN> AAA Setup > Local Users > Add or Edit > VPN Policy > Clientless SSL VPN**，然後從Smart Tunnel List屬性旁邊的下拉選單中選擇智慧隧道名稱。

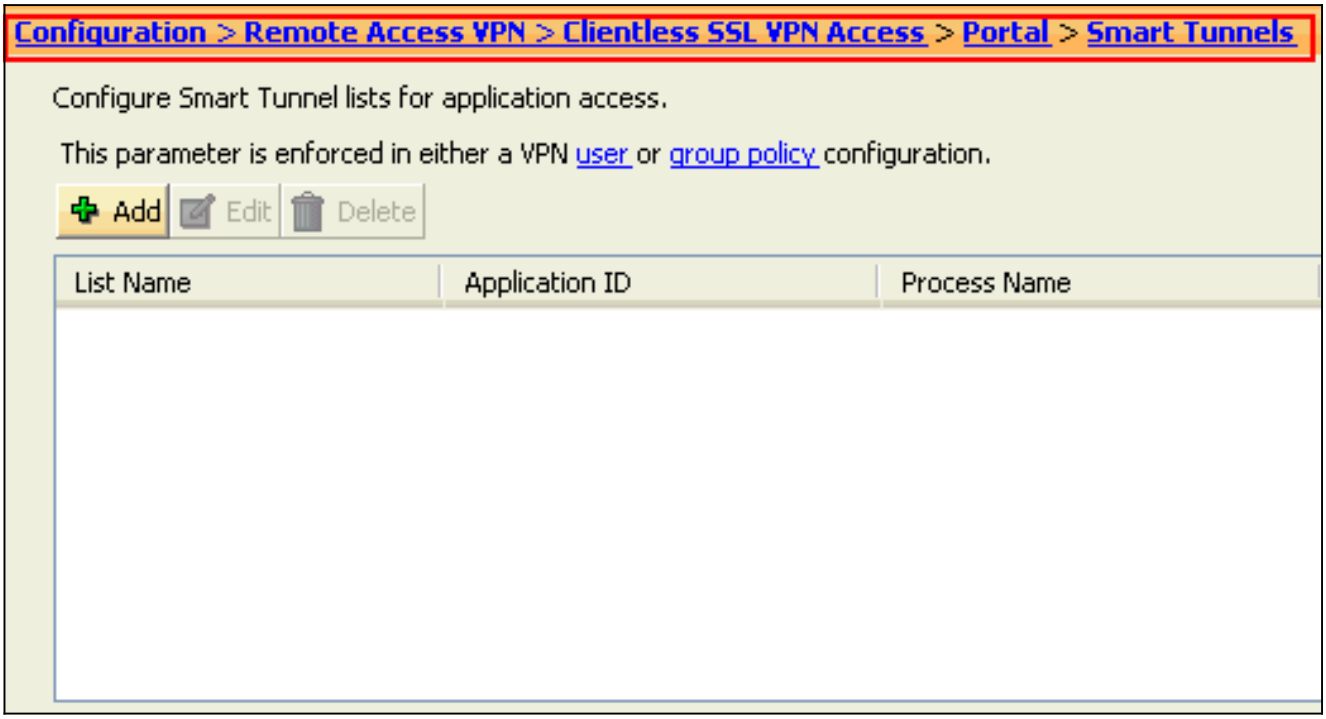
使用ASDM 6.0(2)的ASA智慧隧道（Lotus示例）配置

本檔案假設基本設定（例如介面組態）已完整且運作正常。

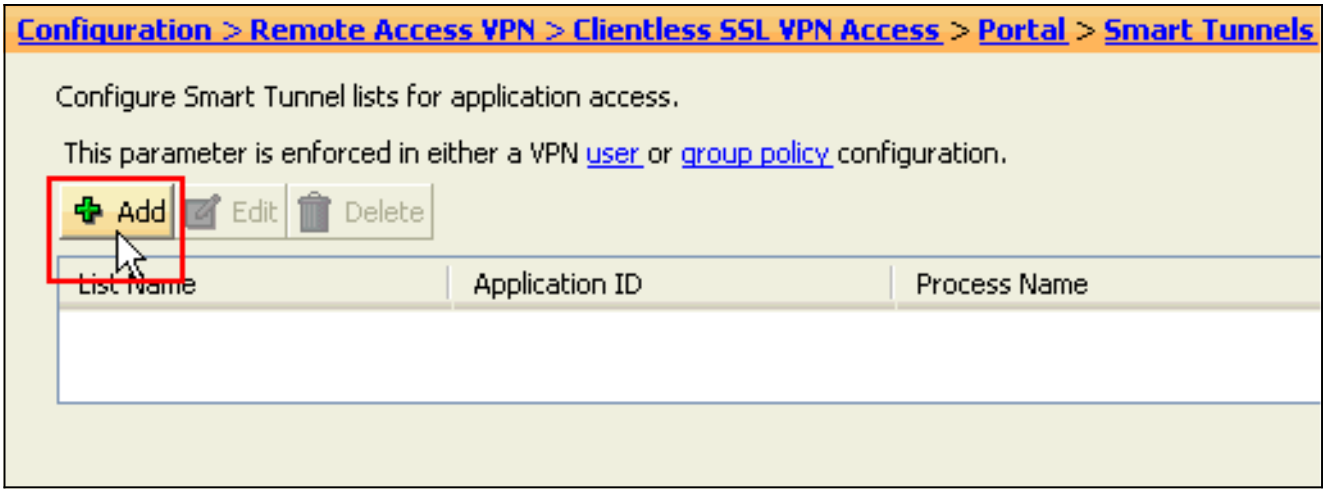
完成以下步驟以設定智慧通道：

注意：在此配置示例中，為Lotus應用程式配置智慧隧道。

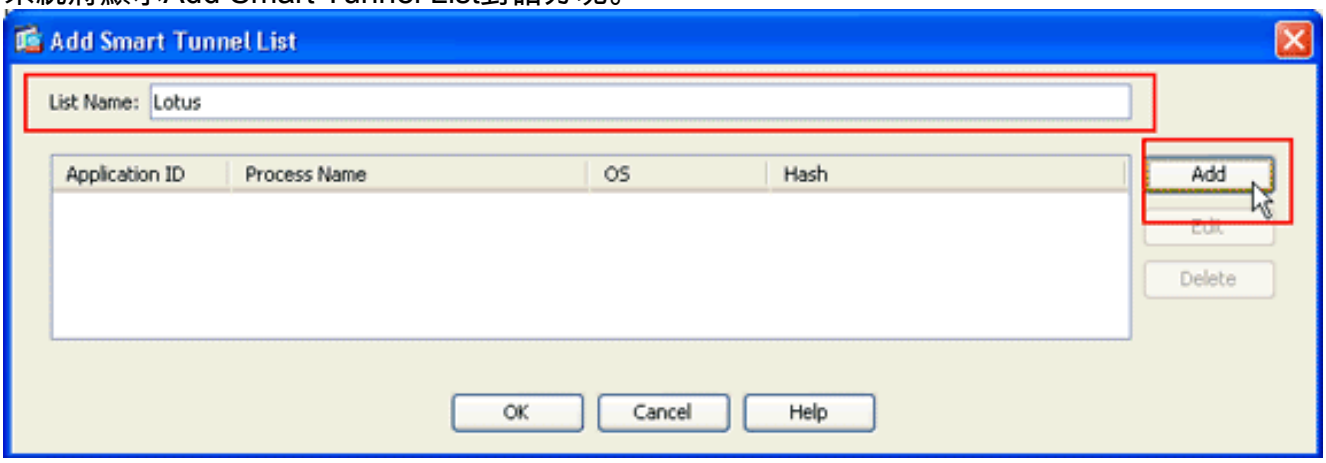
1. 選擇**Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**以啟動智慧隧道配置。



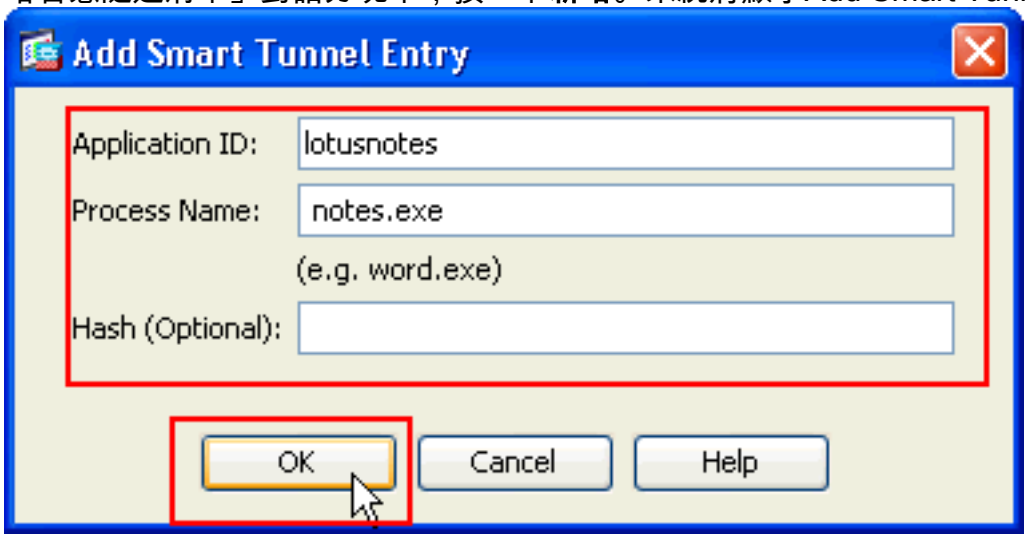
2. 按一下「**Add**」。



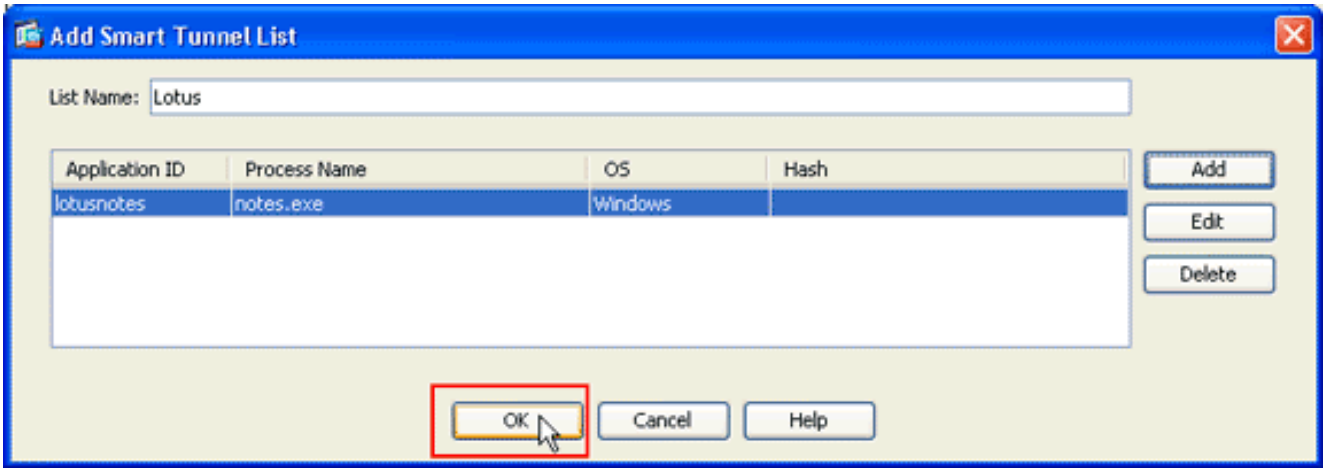
系統將顯示Add Smart Tunnel List對話方塊。



3. 在「新增智慧隧道清單」對話方塊中，按一下**新增**。系統將顯示Add Smart Tunnel Entry對話方塊。

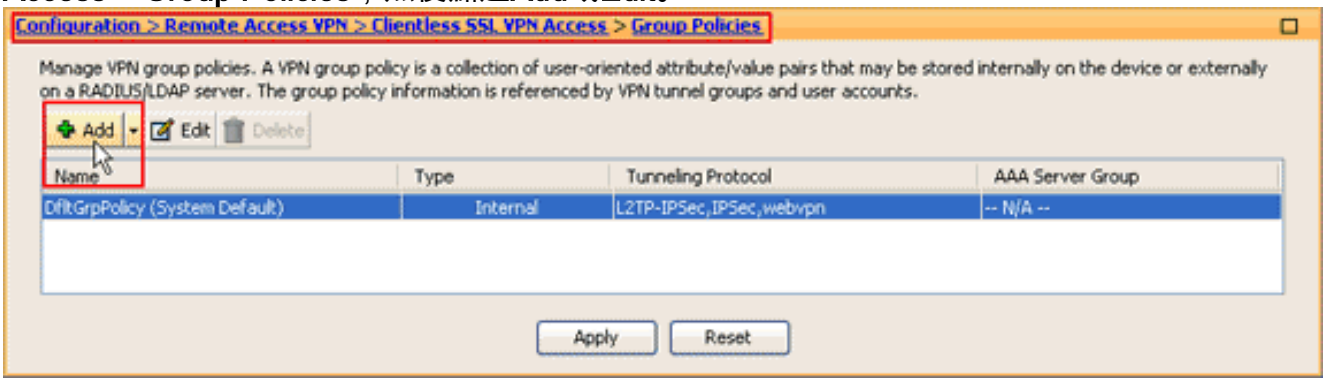


4. 在Application ID欄位中，輸入用於標識智慧隧道清單中的條目的字串。
5. 輸入應用程式的檔名和副檔名，然後按一下**確定**。
6. 在「新增智慧隧道清單」對話方塊中，按一下**確定**。

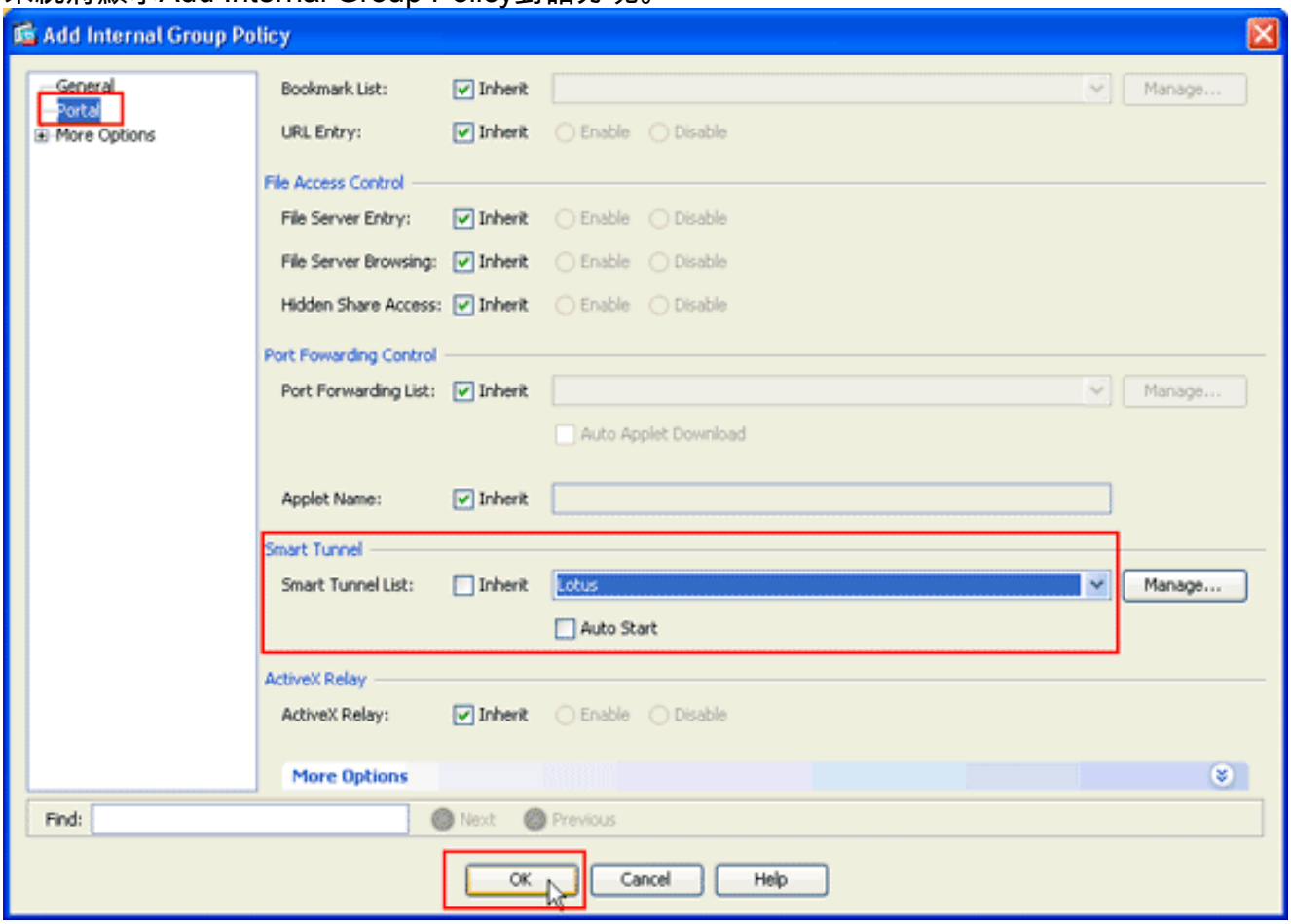


注意：以下是等效的CLI配置命令：

7. 將該清單分配給要向其提供相關應用的智慧隧道訪問的組策略和本地使用者策略，如下所示：要將清單分配給組策略，請選擇**Configuration > Remote Access VPN> Clientless SSL VPN Access > Group Policies**，然後點選**Add**或**Edit**。



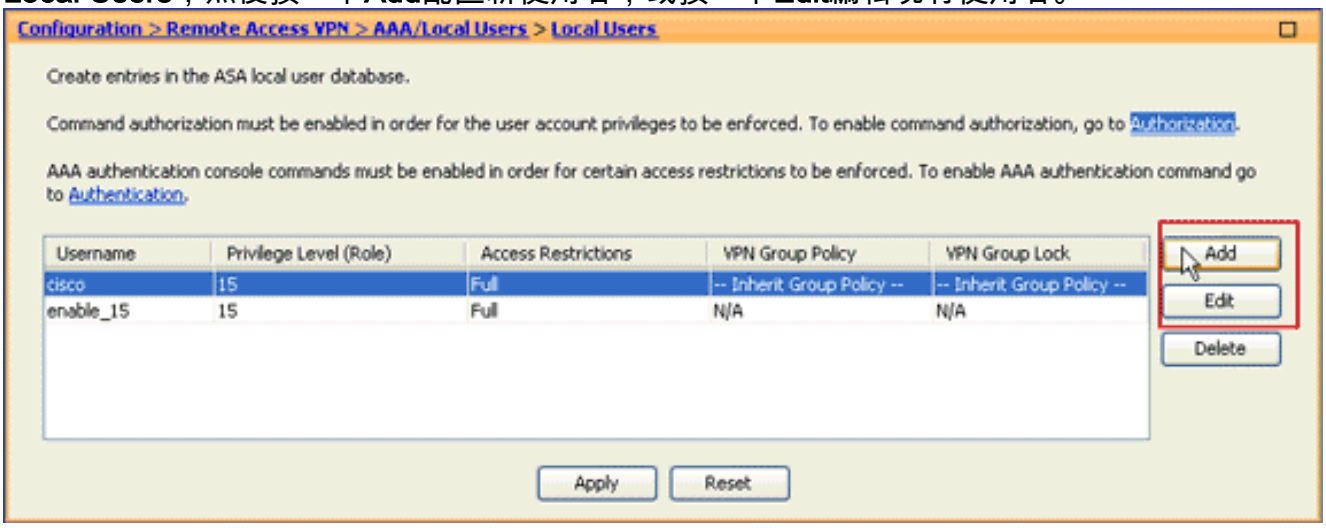
系統將顯示Add Internal Group Policy對話方塊。



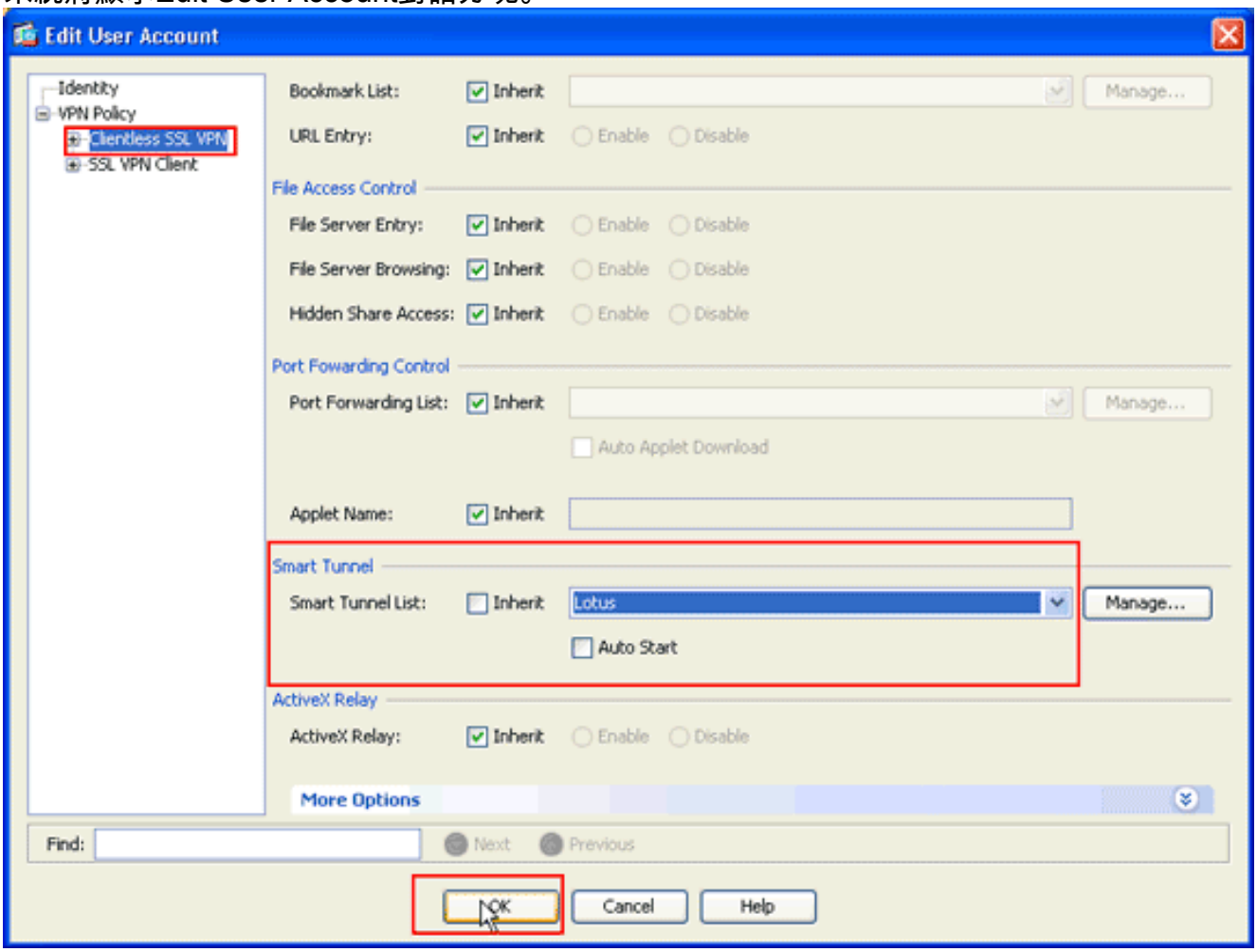
8. 在Add Internal Group Policy對話方塊中，按一下**Portal**，從Smart Tunnel List下拉選單中選擇

智慧隧道名稱，然後按一下**OK**。**注意**：此示例使用*Lotus*作為智慧隧道清單名稱。

9. 要將清單分配給本地使用者策略，請選擇**Configuration > Remote Access VPN> AAA Setup > Local Users**，然後按一下**Add**配置新使用者，或按一下**Edit**編輯現有使用者。



系統將顯示Edit User Account對話方塊。



10. 在「編輯使用者帳戶」對話方塊中，按一下**無客戶端SSL VPN**，從「智慧隧道清單」下拉選單中選擇智慧隧道名稱，然後按一下**確定**。**注意**：此示例使用*Lotus*作為智慧隧道清單名稱。

智慧隧道配置已完成。

疑難排解

無法使用無客戶端門戶中帶書籤的智慧隧道URL進行連線。為什麼會出現此問題，如

何解決此問題？

此問題是由思科錯誤ID CSCsx05766 (僅限註冊客戶)中描述的問題導致的。 為了解決此問題，請將Java Runtime外掛降級為較舊版本。

是否可以查詢WebVPN中配置的智慧隧道連結的URL?

在ASA上使用智慧隧道時，無法查詢URL或隱藏瀏覽器的位址列。使用者可以檢視使用智慧隧道的WebVPN中配置的連結的URL。因此，它們可以更改埠並訪問伺服器以獲取其他服務。

若要解決此問題，請使用WebType ACL。如需詳細資訊，請參閱WebType存取控制清單。

相關資訊

- Cisco ASA 5500系列調適型安全裝置
- 帶ASDM的ASA上的SSL VPN客戶端(SVC)配置示例
- 技術支援與文件 - Cisco Systems